PRODUCT LINE

Integrated Solutions You Can Trust

Deep Protection

SonicWALL® provides Network Security, Secure Remote Access and Continuous Data Protection solutions. These solutions enable organizations of all sizes to secure deep protection without compromising network performance. With easy-to-use, wired and wireless SonicWALL network security solutions, organizations are easily able to take complete control of protecting their network infrastructure utilizing our deep packet inspection firewall technology and advanced security services. SonicWALL's Secure Remote Access solutions enable users to gain safe access to their organization's network 24x7. And, using SonicWALL's Continuous Data Protection solutions, organizations can experience the ease of real-time, continuous, end-to-end data protection for servers, laptops and PCs — without the manual inefficiency and unreliability of tape backup.

SonicWALL solutions are deployed in small and medium businesses as well as distributed enterprise environments, government, retail point-of-sale, healthcare markets and service providers.

Network Security Solutions

Advanced Network Security Services

Each SonicWALL Internet security appliance can be configured into a customized solution with an expanding array of security services designed to integrate seamlessly into a network and provide complete protection. Each appliance is capable of integrating support for gateway anti-virus, anti-spyware, intrusion prevention, enforced desktop anti-virus, content filtering and more. SonicWALL appliances also intelligently enforce and dynamically update each of these services as new updates become available.

All-in-One, Network Security Solutions

All-in-one security solutions are available from SonicWALL and they are based upon deep packet inspection firewall and IPSec VPN technologies with integrated gateway anti-virus, anti-spyware, intrusion prevention, enforced desktop anti-virus and content filtering capabilities. By employing an all-in-one solution for security needs, customers can greatly simplify the management of local, remote and mobile network services while protecting key information and communications resources in a cost-effective manner.

Secure Wireless Networking

Wireless technology has changed the face of the static work environment, enabling unprecedented mobility and productivity gains. With a SonicWALL wireless networking solution, you can deploy the latest 802.11a/b/g technologies to ensure reliable communications, yet protect your organization with our award-winning hardened deep packet inspection firewalls, ensuring that users get enterprise quality wireless security, regardless of the size of your organization.

Secure Remote Access

The SonicWALL suite of VPN solutions provides organizations of all sizes with easy-to-use ways to provide secure access to corporate resources through broadband, wireless and dial-up connections from remote locations. IPSec VPN is integrated in all TZ and PRO Series security appliances. It uses encryption and authentication technology to create a secure, private tunnel through an IP network for site-to-site connections. Or, by integrating a SonicWALL SSL-VPN solution along side an existing firewall, organizations can easily provide mobile workers with secure remote access through a standard Web browser. Because it uses a Web-based interface, there is no need for managing a pre-installed client, making the task of offering remote access a breeze for an already overtaxed IT staff.

Continuous Data Protection

Real-time, Tapeless, Data Protection

SonicWALL Continuous Data Protection (CDP) solutions provide automatic, real-time data backup for servers, laptops and PCs. The solution protects files first locally to ensure files from any previous point in time can be recovered – instantly. It also includes hands-free, automatic offsite capabilities to protect businesses against disasters. And, since SonicWALL CDP only backs up block level differences within each file, the network is not impacted or compromised. Importantly, central management and remote administration features allow IT administrators to operate efficiently and effectively.

SONICWALL

A Recognized Leader in Network Security and Continuous Data Protection Solutions

From our founding in 1991, SonicWALL, Inc. has been dedicated to our customers' needs, believing appliances can and should perform multiple functions—especially those that sit at the gateway. And we were the first to integrate additional capabilities into a firewall appliance, including VPN and content filtering.

Today, we have emerged as a leader in network security and continuous data protection with offerings like our market leading Unified Threat Management solutions, with enterprise-class, appliance-based products and services that provide anti-virus, intrusion prevention and anti-spyware, for wired and wireless networks of all sizes, in a single package. More than 650,000 SonicWALL security appliances have shipped to protect millions of computer users in small, medium and distributed networks, enterprise, e-commerce, education, healthcare, retail/point-of-sale and government markets from a wide range of security threats, while improving network productivity.

SonicWALL's commitment to this market is about more than products: it encompasses all the resources and ongoing vision it takes to keep network security and data protection solutions ahead of ever-evolving threats. SonicWALL strategic partners are some of the best-known names in information technology and serve the global market with over 15,000 qualified, customer-focused resellers and distributors. SonicWALL's commitment to the channel has been validated for the second year running with the VAR Business 5-Star Partner Program award and the VAR Business ARC awards for Best Overall Vendor, Security Appliances, receiving top marks for Product Innovation, Partnering and Loyalty. SonicWALL provides comprehensive technical support, and maintains the finest team of security and data protection professionals in the industry, devoted to continuous innovation in integrated network security and data protection solutions.

Advanced Security Services

SonicWALL

GAV/ Anti-Spyware/ IPS

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service

SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers intelligent, real-time network security protection against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans and software vulnerabilities such as buffer overflows, as well as backdoor exploits and other malicious code. As an added layer of security, this powerful solution provides application layer attack protection not only against external threats, but also against those originating inside the network. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service closes potential backdoors by inspecting over a multitude of e-mail, Web, file transfer and stream-based protocols as well as instant messaging (IM) and peer-to-peer (P2P) applications.

- Per packet scanning engine handles unlimited file sizes and virtually hundreds of thousands of concurrent downloads
- Enforce intrusion prevention and anti-virus scanning not only between each network zone and the Internet, but also between internal network zones
- Dynamically updated database contains thousands of attack, vulnerability, IM and P2P signatures

SonicWALL

Content Filtering Service

SonicWALL Content Filtering Service

SonicWALL Content Filtering Service (CFS) provides businesses and schools with greater control to transparently enforce productivity and protection policies and block inappropriate, illegal and dangerous Web content. Featuring a dynamic rating and caching architecture, SonicWALL CFS blocks multiple categories of objectionable Web content, providing the ideal combination of control and flexibility to ensure the highest levels of productivity and protection.

- Scalable, enterprise-class content filtering for networks of all sizes
- Web site caching for seamless response to frequently-visited sites
- Innovative rating architecture provides greater control to enforce protection and productivity policies

SonicWALL

Complete Anti-Virus

SonicWALL Network Anti-Virus and SonicWALL Complete Anti-Virus

Developed in partnership with McAfee®, SonicWALL Network Anti-Virus delivers enforced and auto-updated desktop protection through automatic system-wide updates of virus definitions, eliminating the need for time-consuming machine-by-machine anti-virus deployments. Combining the enforced desktop security in SonicWALL Network Anti-Virus with advanced server protection, SonicWALL Complete Anti-Virus leverages the award-winning McAfee NetShield® and GroupShield™ applications for networks with Windows®-based file, print and Exchange servers. By delivering very fast time-to-response during rapid virus outbreaks, SonicWALL anti-virus solutions reduce the time and costs associated with administering an anti-virus policy throughout your entire network.

- Auto-enforcement of anti-virus policy for always-on virus protection
- Advanced heuristics and early warning alerts for fast time-to-protection
- Rapid e-mail attachment blocking for the fastest protection from malicious viruses

SonicWALL

Global Security Client

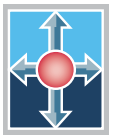
SonicWALL Global Security Client

The SonicWALL Global Security Client combines personal firewall software and the SonicWALL Global VPN Client in a single, easy-to-use solution, extending comprehensive desktop security to mobile workers and corporate networks. Central policy configuration, distribution and management at the gateway greatly improves employee productivity and network efficiency while preventing the use of inappropriate and unproductive applications. The Global Security Client provides network administrators with the tools to configure and distribute granular policies by IP address or operating system for added flexibility.

- Seamless creation, distribution and management of global security policies
- Protection for corporate networks and remote/mobile workers from malicious attacks
- Global VPN Client provides mobile users with secure, reliable access to corporate resources through broadband, wireless and dial-up connections

Firmware

SonicWALL



SonicOS Enhanced

SonicOS Enhanced Firmware

SonicOS Enhanced is the powerful next-generation operating system from SonicWALL, offering a host of advanced features to meet the business continuity, configuration flexibility and management requirements of complex networks today and into the future. Available as an optional upgrade on the PRO 3060, PRO 2040, PRO 1260, TZ 170 Wireless, TZ 170 SP and TZ 170, SonicOS Enhanced comes standard with the PRO 5060, PRO 4100, PRO 4060, PRO 1260 Enhanced and TZ 170 SP Wireless, providing superior networking and security features to maximize the capabilities of your SonicWALL appliance.

- ISP failover and load balancing for highly reliable network connectivity and robust performance
- Object and zone-based management simplify implementing and managing security policies
- Advanced routing services ensure network route availability and easy integration with existing routing infrastructures

SonicWALL PRO Series At-A-Glance

The SonicWALL PRO Series is a multi-service security platform for companies requiring rock solid network protection coupled with fast, secure VPN access for remote employees. Built on the innovative SonicWALL deep packet inspection architecture, the PRO Series combines gateway anti-virus, anti-spyware, intrusion prevention, anti-spam and content filtering capabilities with a deep packet inspection firewall and IPSec VPN for real-time, granular protection against malicious application layer attacks. With six distinct, highly integrated security appliances, the PRO Series delivers the scalability and performance growing networks require.

Every PRO Series appliance packs the benefits of the SonicWALL SonicOS operating system into an affordable, rack-mount appliance, providing enterprise-class performance, advanced features and configuration flexibility. Standard on the PRO 4060/4100/5060 and an optional upgrade on the PRO 1260/2040/3060, feature-rich SonicWALL SonicOS Enhanced adds a suite of redundancy, management and wireless LAN features typically associated with more expensive appliances including Quality of Service (QoS), ISP failover, WAN redundancy, load balancing, object/zone-based management, policy-based NAT, wireless guest services and more.

PRO Series appliances are ICSA-certified and can be easily managed remotely as part of a multi-firewall and VPN environment through a Web interface or using the industry-leading SonicWALL Global Management System (GMS).

Real-time unified threat management provides deep protection

Feature	PRO 1260	PRO 2040	PRO 3060	PRO 4060	PRO 4100	PRO 5060
Nodes			Unrestricted			
Interfaces	27 Ethernet	3/4* Ethernet	3/6* Ethernet	6 Ethernet	10 Gigabit	6 Gigabit
SonicOS Standard/Enhanced	Either	Standard	Standard	Enhanced	Enhanced	Enhanced
Upgrade to SonicOS Enhanced	Yes	Yes	Yes	N/A	N/A	N/A
Stateful Throughput[1]	90 Mbps	200 Mbps	300 Mbps	300+ Mbps	800 Mbps	2.4 Gbps
Gateway Anti-Virus Throughput[2]	8 Mbps	40 Mbps	99 Mbps	182 Mbps	300 Mbps	339 Mbps
Intrusion Prevention Throughput[2]	8 Mbps	39 Mbps	98 Mbps	170 Mbps	300 Mbps	279 Mbps
Connections	10,000	32,000	128,000	500,000	600,000	750,000
Policies	150/300*	150/1,000*	300/3,000*	5,000	10,000	15,000
3DES/AES Throughput[3]	30+ Mbps	50 Mbps	75 Mbps	190 Mbps	350 Mbps	700 Mbps
Site-to-Site VPN Tunnels	25	50	500/1,000*	3,000	3,500	4,000
Remote Access VPN Tunnels (Max)	50	100	500	3,000	5,000	6,000
Remote Access VPN Tunnels (Bundled)	5	10	25	1,000	1,500	2,000
Zone Security	Yes*	Yes*	Yes*	Yes	Yes	Yes
Object-based Management	Yes*	Yes*	Yes*	Yes	Yes	Yes
Policy-based NAT	Yes*	Yes*	Yes*	Yes	Yes	Yes
WAN/WAN Failover	Yes*	Yes*	Yes*	Yes	Yes	Yes
ISP Failover	Yes*	Yes*	Yes*	Yes	Yes	Yes
Load Balancing	Yes*	Yes*	Yes*	Yes	Yes	Yes
Hardware Failover	No	Yes*	Yes*	Yes	Yes	Yes
Wireless LAN Services	Yes*	Yes*	Yes*	Yes	Yes	Yes
Spam Blocking	Yes*	Yes*	Yes*	Yes	Yes	Yes
Voice over IP (VoIP)	Yes	Yes	Yes	Yes	Yes	Yes

**With SonicOS Enhanced upgrade*
[1]Firewall throughput measured using UDP traffic at 1518 byte packet size adhering to RFC 2544
[2]Gateway AV/Anti-Spyware/IPS throughput measured using HTTP traffic
[3]VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544

SonicWALL PRO 5060

The PRO 5060 is an enterprise-class, multi-service, gigabit network security platform that protects users and critical network resources from the dynamic, sophisticated threats that put today's corporate networks at risk. Available in 10/100/1000 copper and copper/fiber interface configurations, the PRO 5060 incorporates advanced networking and security features such as such as 802.1q virtual LANs, dynamic RIP and OSPF routing, Quality of Service (QoS) and more, making it an ideal solution for data-intensive network environments. The PRO 5060 includes SonicWALL ViewPoint® reporting software, one year of Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service and 2,000 Global VPN Client licenses for secure remote access.

SonicWALL PRO 4100

The PRO 4100 is an enterprise-class unified threat management platform that delivers real-time internal and external network protection to corporate networks, distributed environments and data centers. The PRO 4100 combines high-speed gateway anti-virus, anti-spyware, intrusion prevention and powerful deep packet inspection capabilities with an extensive array of advanced networking and configuration flexibility features in an accessible, affordable platform that is easy to deploy and manage. With 10 configurable gigabit Ethernet interfaces, SonicWALL Clean VPN technology and built-in secure wireless LAN functionality, the PRO 4100 is an ideal solution for a host of wired and wireless applications requiring high-speed access and heavy workgroup segmentation.

SonicWALL PRO 4060

The PRO 4060 is a high-performance, multi-service network security platform designed to meet the critical security requirements of medium-to-large sized networks. With 190 Mbps of hardware-accelerated VPN performance, enhanced VPN capabilities and 1,000 Global VPN Client licenses, the PRO 4060 is the ideal solution for even the most complex remote connectivity environments. Six configurable 10/100 Ethernet interfaces allow administrators to create multiple LANs, WANs, WLANs, DMZs and custom-defined zones for greater network configuration flexibility. The PRO 4060 includes SonicWALL ViewPoint reporting software and 1,500 Global VPN Client licenses for secure remote access.

SonicWALL PRO 3060

The PRO 3060 is a high-performance, network security platform designed to meet the business continuity needs of mid-sized networks. Powered by the SonicWALL next-generation SonicOS operating system, the PRO 3060 delivers powerful firewall throughput and 3DES/AES VPN concentration. An upgrade on the PRO 3060, SonicOS Enhanced unlocks critical redundancy features such as hardware failover, WAN/ISP failover and the ability to fail over to a secondary VPN gateway, ensuring continuous network uptime. Six configurable 10/100 Ethernet interfaces allow administrators to create multiple LANs, WANs, WLANs, DMZs and custom-defined zones for greater network configuration flexibility.

SonicWALL PRO 2040

The PRO 2040 is an award-winning network security platform designed to meet the business continuity needs of small-to-mid sized networks. Optimized for networks of up to 200 nodes or 50 network locations, the PRO 2040 delivers powerful firewall throughput and 3DES/AES VPN concentration. An upgrade on the PRO 2040, SonicOS Enhanced provides hardware failover, WAN/ISP failover and the ability to fail over to a secondary VPN gateway, ensuring continuous network uptime. Four configurable 10/100 Ethernet interfaces allow administrators to create multiple LANs, WANs, WLANs, DMZs and custom-defined zones for greater network configuration flexibility.

SonicWALL PRO 1260

The PRO 1260 is a total security and switching platform for small network applications. The PRO 1260 combines deep packet inspection firewall and IPSec VPN capabilities with an intelligent, wire-speed, 24-port auto-sensing MDIX switch in a single, convenient network security and LAN switching platform. This unique appliance can be configured either as an unmanaged switch under SonicOS Standard or as an intelligent managed LAN switching platform through the powerful SonicWALL PortShield architecture enabled in SonicOS Enhanced. The innovative PortShield architecture allows all 24 ports on the PRO 1260 to be independently and easily configured into custom security zones (PortShield groups), each with its own "virtual firewall," along with granular rate limiting on each interface.

SonicWALL TZ Series At-A-Glance

The SonicWALL TZ Series is the ideal total security platform for home, small and remote/branch offices, providing a compelling blend of ease-of-use for basic networks and unsurpassed flexibility for more complex networks. Integrating deep packet inspection firewall, 802.11b/g secure wireless, failover/failback, gateway anti-virus, anti-spyware, intrusion prevention, content filtering, and IPSec VPN capabilities into an affordable solution, the TZ Series scales to protect your investment as your organization grows. Available in multiple hardware and node configurations, the TZ Series allows you to add features and functionality when your network needs them.

Every TZ Series appliance packs the benefits of SonicWALL SonicOS operating system into an affordable desktop appliance, providing business-class performance, advanced features and configuration flexibility. Standard on the TZ 170 SP Wireless and an optional upgrade on all other TZ 170 Series appliances, the SonicWALL feature-rich SonicOS Enhanced adds a suite of redundancy, management and wireless LAN features typically associated with more expensive appliances including ISP failover, load balancing, object/zone-based management, policy-based NAT, wireless guest services and more.

TZ Series appliances are ICSA-certified and can be easily managed remotely as part of a multi-firewall and VPN environment through a Web interface or using the industry-leading SonicWALL Global Management System (GMS).

TZ 170 Series is the ultimate total security platform for small networks, including remote and branch offices and retail/POS deployments

Feature	TZ 150	TZ 150 Wireless	TZ 170	TZ 170 Wireless	TZ 170 SP	TZ 170 SP Wireless
Nodes	10	10	10/25/Unrestricted		10	10
Interfaces	5 Ethernet	5 Ethernet	7 Ethernet	7 Ethernet	7 Ethernet	7 Ethernet
SonicOS Standard/Enhanced	Standard	Standard	Standard	Standard	Standard	Enhanced
Upgrade to SonicOS Enhanced	No	No	Yes	Yes	Yes	N/A
Stateful Throughput[1]	30 Mbps	30 Mbps	90 Mbps	90 Mbps	90 Mbps	90 Mbps
Gateway Anti-Virus Throughput[2]	8 Mbps	8 Mbps	8 Mbps	8 Mbps	8 Mbps	8 Mbps
Intrusion Prevention Throughput[2]	8 Mbps	8 Mbps	8 Mbps	8 Mbps	8 Mbps	8 Mbps
Connections	2,000	2,000	6,000	6,000	6,000	6,000
Policies	20	20	100/250*	100/250*	100/250*	100/250*
3DES/AES Throughput[3]	10+ Mbps	10+ Mbps	30+ Mbps	30+ Mbps	30+ Mbps	30+ Mbps
Site-to-Site VPN Tunnels	2	2	2/10/10	2/10/10	2	2
Remote Access VPN Tunnels (Max)	2	2	5/50/50	5/50/50	5	5
Remote Access VPN Tunnels (Bundled)	Optional Upgrade		Optional Upgrade/1/1		Optional Upgrade	
Zone Security	No	No	Yes*	Yes*	Yes*	Yes
Object-based Management	No	No	Yes*	Yes*	Yes*	Yes
Policy-based NAT	No	No	Yes*	Yes*	Yes*	Yes
WAN/WAN Failover	No	No	Yes*	Yes*	Yes*	Yes
ISP Failover	No	No	Yes*	Yes*	Yes*	Yes
Load Balancing	No	No	Yes*	Yes*	Yes*	Yes
Wireless LAN Services	No	No	Yes*	Yes*	Yes*	Yes
Integrated Access Point	No	Yes	No	Yes	No	Yes
Receive Power over Ethernet	No	No	No	Yes	No	Yes
Integrated Analog Modem	No	No	No	No	Yes	Yes
Optional Port	No	No	Yes	Yes	Yes	Yes
Spam Blocking	No	No	Yes*	Yes*	Yes*	Yes
Voice over IP (VoIP)	Yes	Yes	Yes	Yes	Yes	Yes

**With SonicOS Enhanced upgrade*

[1]Firewall throughput measured using UDP traffic at 1518 byte packet size adhering to RFC 2544

[2]Gateway AV/Anti-Spyware/IPS throughput measured using HTTP traffic

[3]VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544

SonicWALL TZ 170 SP Wireless

The TZ 170 SP Wireless is a total wired and wireless security platform ensuring continuous network uptime through integrated and automated failover and failback technologies. Dual broadband WAN connections plus an integrated analog modem and secure 802.11b/g wireless make the TZ 170 SP Wireless the first appliance to offer automated broadband-to-broadband-to-analog WAN redundancy for unparalleled uptime on both wired and wireless networks. The TZ 170 SP Wireless comes standard with the feature-rich SonicWALL SonicOS Enhanced firmware which includes advanced networking and security features including ISP failover, zone and object-based management, policy-based routing, NAT, spam blocking and more.

SonicWALL TZ 170 SP

The TZ 170 SP is a total security platform for telecommuters and point-of-sale businesses that ensures continuous network uptime for critical, secure data connectivity through integrated and automated failover and failback technologies. With an integrated analog modem and an optional port that can be configured as a second WAN through SonicOS Enhanced, the TZ 170 SP offers automated broadband-to-broadband-to-analog WAN redundancy for unparalleled network uptime.

SonicWALL TZ 170 Wireless

The TZ 170 Wireless is a total security platform delivering business-class wireless and wired security to small networks through integrated secure 802.11b/g wireless, firewall and VPN technologies in a cost-effective, easy-to-use solution. Advanced features such as enforced VPN encryption on the wireless LAN, plus wireless intrusion and rogue access point detection, deliver impenetrable wireless security. The TZ 170 Wireless provides network administrators with the ability to create multiple zones of access—for wired and wireless workers as well as guest wireless users—offering an unprecedented level of control without compromising network security.

SonicWALL TZ 170

The TZ 170 is a total security platform for small, remote and branch office networks, featuring an integrated 5-port, auto-sensing MDIX switch and configurable optional port. Upgrading to SonicOS Enhanced enables the optional port to be configured as a workport for telecommuters, a second WAN for ISP failover and load balancing, a second LAN or another custom-defined zone for added network flexibility. This high-performance deep packet inspection firewall comes standard with bundled VPN Client licenses* for secure remote access.

**VPN Client licenses bundled with 25 and Unlimited node versions*

SonicWALL TZ 150 Wireless

The TZ 150 Wireless is a complete layered security platform integrating secure 802.11b/g wireless and a deep packet inspection firewall in an easy-to-use, low cost platform. The compact form factor includes a single Ethernet WAN port and four-port auto-MDIX LAN switch, allowing multiple devices to connect safely to the network. Advanced features such as enforced VPN encryption on the wireless LAN and wireless intrusion detection and prevention services deliver impenetrable wireless security. Utilizing the wireless guest services feature, network administrators can create multiple zones of access—for wired and wireless workers as well as guest wireless users—offering an unprecedented level of control without compromising network security.

SonicWALL TZ 150

The TZ 150 delivers layered protection to small and home offices through an integrated deep packet inspection firewall in an easy-to-use, low cost platform. The compact form factor includes a single Ethernet WAN port and four-port auto-MDIX LAN switch, allowing multiple devices to connect safely to the network. The TZ 150 supports hardware-accelerated IPSec 3DES and AES encryption as well as SonicWALL Global VPN Client upgrades for secure remote access to critical network resources.

Content Security Management Solutions

SonicWALL Content Security Manager 2100 CF

The SonicWALL Content Security Manager 2100 Content Filter (CSM 2100 CF) is an appliance-based Internet filtering solution that integrates real-time gateway anti-virus, anti-spyware and Internet filtering to deliver maximum network protection from today's sophisticated Internet threats. Combining dynamic threat management capabilities with precise control over Internet usage in an affordable, appliance-based solution, the CSM 2100 CF boosts network security and employee productivity, optimizes network utilization and mitigates legal liabilities. This unique solution integrates seamlessly into virtually any network topology for powerful, scalable and cost-effective threat protection.

- Blocks continually-evolving threats including viruses, worms, Trojans, spyware, keyloggers, phishing and malicious mobile code (MMC)
- Granular controls for managing access to Web sites containing unproductive and potentially illegal Web content
- Instant messaging, peer-to-peer and multimedia application controls enhance bandwidth utilization
- Dynamically updated signature and ratings databases ensure vulnerabilities are blocked before they can be exploited
- Advanced reporting and analysis tool provides insight into network usage through custom reports

Secure Wireless Solutions

SonicWALL Secure Wireless Solution

The SonicWALL Secure Wireless Solution is the first wireless networking security solution that integrates 802.11a/b/g wireless management and security enforcement into an enterprise-class firewall/VPN gateway. The innovative SonicWALL Secure Wireless Solution scales to fit virtually any network deployment by simply distributing SonicPoints™ at optimal locations throughout the building. Available in IEEE 802.11a/b/g and 802.11/b/g options, SonicPoints are dependent access points that are utilized to provide seamless, secure wireless LAN (WLAN) connectivity as well as advanced features and services. SonicPoints can receive 802.3af power over Ethernet (PoE) to aid in their convenient deployment in any network. The Secure Wireless Solution is built around the SonicWALL award-winning TZ 170 and PRO Series security appliances which function as secure wireless switches and controllers, automatically detecting and configuring SonicPoints as they are added to the network while simultaneously enforcing security policies on all wired and wireless traffic.

- IEEE 802.11a/b/g compliance allows interoperability with any standards-compliant 802.11a/b/g wireless clients
- Wireless guest services provide guests with wireless Internet-only access without compromising the corporate network
- Advanced WLAN security including enforced VPN encryption on the wireless LAN and wireless intrusion detection and prevention
- SonicWALL PoE Injector feeds remote power directly to the SonicPoint through a standard Ethernet cable
- SonicWALL Long Range Dual Band Wireless Card delivers superior data transmission and reception at extended ranges for maximum data integrity

SonicWALL SSL-VPN Series

The SonicWALL SSL-VPN Series provides organizations with an affordable, simple and secure clientless remote network and application access solution that requires no pre-installed client software. Utilizing only a standard Web browser, users can easily and securely access e-mail, files, intranets, applications, remote desktops, servers and other resources on the corporate LAN from any location. SonicWALL SSL-VPN solutions integrate seamlessly into virtually any wired or wireless network topology to deliver powerful, scalable and affordable remote access to corporate resources.

- Offering unrestricted concurrent user tunnels instead of per-tunnel licensing significantly reduces the costs associated with deploying a scalable secure remote access solution
- Clientless connectivity frees administrators from the tedious and costly task of installing and updating a client on a user's PC
- Granular policy configuration controls enable administrators to create policies that "lock down" users to specific applications/resources
- Enhanced layered security is provided when deployed alongside a SonicWALL Internet security appliance utilizing powerful deep packet inspection technology
- NetExtender technology provides enhanced capabilities such as access to additional resources, services and applications on the corporate network

SonicWALL SSL-VPN 2000

The SonicWALL SSL-VPN 2000 provides mid-size organizations with a simple, affordable secure and clientless remote network and application access solution for remote and mobile employees.

SonicWALL SSL-VPN 200

The SonicWALL SSL-VPN 200 provides small organizations with a simple, clientless, cost effective alternative to traditional remote access and remote control software products.

SonicWALL CDP Series At-A-Glance

The SonicWALL Continuous Data Protection (CDP) solution is a tapeless, enterprise-level back-up and recovery appliance that provides deep protection for businesses and remote offices. This hands-free, disk-based data protection solution provides automatic continuous data backup for servers, laptops and PCs—locally and offsite. By combining the advantages of local disk-based backup (instant recovery) with offsite backup (insurance against local disasters), the SonicWALL CDP Series is the first solution to eliminate, not just mitigate, exposure to threats of data loss. The solution also includes central management and remote administration features that enable IT administrators to more effectively and efficiently protect an organization's data.

Continuous real-time data protection with local and offsite backup

Feature	CDP 1440i	CDP 2440i	CDP 3440i	CDP 4440i
Core Compression Technology	Standard	Standard	Enhanced	Enhanced
Encryption	AES 256-bit	AES 256-bit	AES 256-bit	AES 256-bit
Throughput	Standard	Standard	Accelerated	Accelerated
Users	15 or fewer	30 or fewer	75 or fewer	Unlimited
Servers	3	5	Unlimited	Unlimited
Base Capacity[1]	160 GB	250 GB	400 GB	600 GB
Compressed Capacity[2]	192 GB	250 GB	600 GB	1.2 TB
Chassis	Mini	Mini	1U Rack	2U Rack
RAID	N/A	N/A	RAID 1	RAID 5
Continuous Data Protection	Yes	Yes	Yes	Yes
File Versions	Yes	Yes	Yes	Yes
Central Administration	Yes	Yes	Yes	Yes
Desktop Laptop, Server Backup	Yes	Yes	Yes	Yes
Remote Administration	Yes	Yes	Yes	Yes
Open Files Backup	Yes	Yes	Yes	Yes
Policy Based Backup	Yes	Yes	Yes	Yes
Active Directory Backup	No	Yes	Yes	Yes
SQL Server Support	No	Yes	Yes	Yes
MS Exchange Server Support	No	Yes	Yes	Yes

[1]Product capacity specified in gigabytes (GB) are terabytes (TB) where 1 GB = 1,000,000,000 bytes and 1 TB = 1,000,000,000,000 bytes.
[2]Compressed capacity assumes 1:2:1 for standard data compression and 2:1 for enhanced data compression. Capacity may vary and is data dependent.

Continuous Data Protection Appliance – CDP Series

SonicWALL CDP 1440i

The CDP 1440i is a disk-based backup and recovery appliance that offers real-time end-to-end data protection for small businesses. It includes unique features such as instant data recovery and central administration. The CDP 1440i supports servers, PCs and laptops for small business networks and up to 15 users, 192 GB compressed capacity and AES 256-bit encryption for offsite data security.

SonicWALL CDP 2440i

The CDP 2440i is ideal for small businesses and remote offices. Featuring a 300 GB compressed capacity along with standard throughput and AES 256-bit encryption for offsite data security, it provides continuous real-time data protection for servers, laptops and PCs. Differentiating this solution from many of its competitors is its seamless support of most small business databases and applications such as SQL-Server and Microsoft Exchange without the need to integrate additional software packages.

SonicWALL CDP 3440i

The CDP 3440i offers enterprise-class data backup protection for small-to-medium businesses and remote offices. The high-performance 1U rack-mountable solution is optimized for up to 75 users and unlimited servers. Offering 600 GB compressed capacity with RAID 1 along with accelerated throughput and AES 256-bit encryption for offsite data security; it provides continuous real-time data protection for servers, laptops and PCs using policy-based backup, central administration and open file backup. It supports most small business databases and applications such as Microsoft Exchange, SQL-Server, Quickbooks, PeachTree, Great Plains, etc.

SonicWALL CDP 4440i

The CDP 4440i is a robust 2U rack-mountable backup and recovery solution for branch offices and mid-size organizations. Offering a 1.2 TB compressed capacity with RAID 5 along with accelerated throughput and AES 256-bit encryption for offsite data security, along with all the features of the CDP 3440i, it provides continuous real-time data protection for unlimited servers, laptops, PCs, databases and business applications. IT Administrators benefit from central management and file-level visibility into every client machine connected to the SonicWALL CDP appliance, enabling enforcement of consistent backup policies and control features available to individual end users.

SonicWALL CDP Offsite Service

The CDP Offsite Service provides an offsite backup and recovery solution that stores the data in a secure data center that enables enterprises to be up and running quickly after a disaster event. All data is securely transmitted and encrypted with an AES 256-bit encryption key. IT Administrators can recover the data through a simple interface in the event that the CDP unit at the local level is not viable.

Security Management and Reporting Solutions

SonicWALL

Global Management System

SonicWALL Global Management System

SonicWALL Global Management System (GMS) provides distributed businesses and service providers with a flexible, powerful and intuitive tool to deploy, manage and monitor a distributed networked environment from a central location. Organizations can globally manage and collect detailed information from security applications such as gateway anti-virus, anti-spyware, intrusion prevention and content filtering, all from a single console. SonicWALL GMS enables organizations to reduce staffing requirements, speed up deployment and lower costs.

- Simplifies configuration and enforcement of global security and VPN policies
- Offers centralized reporting and monitoring of firewall and network activities
- Scales to support growing deployments

SonicWALL

ViewPoint

SonicWALL ViewPoint

SonicWALL ViewPoint is a Web-based graphical reporting tool that provides administrators with unprecedented security awareness and control over their network environments through detailed and comprehensive reports of network and firewall activities, including firewall attacks, bandwidth usage, Web site visits, user activity and more.

- Graphical, easy-to-interpret reports on network and security activities
- On-demand reporting saves administrative overhead
- Web interface simplifies deployment and access from a local or remote system

SonicWALL Dynamic Support Services

SonicWALL

Dynamic Support Services

SonicWALL Dynamic Support 8x5 and 24x7

SonicWALL Dynamic Support Services help you maximize your SonicWALL investment not only by keeping your security infrastructure current, but also by reacting swiftly to any problem that may occur. Because support is more than just a break-fix service, our support services provide crucial firmware updates and upgrades filled with new features and capabilities. To help you implement these, our services also include timely access to a comprehensive set of electronic tools and information.

- Firmware updates and upgrades maintain network security and maximize your SonicWALL investment
- Quick access to support, ensuring your mission-critical systems are safe
- Simple, comprehensive offerings that let you plan your annual costs

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

SONICWALL

©2006 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. BRU-01/06